What is claimed is:

1. A method of performing radix 2^N (N>1) Montgomery multiplication, comprising;

receiving a multiplicand, a modulus, and a multiplicator;

performing accumulation in carry save mode on a plurality of inputs related to the multiplicand, modulus, and multiplicator to generate a result in redundant representation; and

performing conversion in carry propagation mode on the result in redundant representation to generate a result in normal representation.

2. A multiple modulus selector comprising:

a modulus recoder for receiving an n-bit modulus M, a previous sum, and a current partial product to generate a first selection signal;

a modulus selector for receiving the n-bit modulus M, the previous sum, the current partial product, and a multiplicand to generate a second selection signal; and

a multiplexer for receiving inputs –M, 0, M, and 2M and selecting one of the inputs based on the first selection signal in an integer modular multiplication mode and selecting one of the inputs based on the second selection signal in a polynomial modular multiplication mode.

3. The multiple modulus selector as recited in claim 2, wherein the input –M is obtained by inverting the modulus M.

4. The multiple modulus selector as recited in claim 2, wherein the input –2M is obtained by shifting the modulus M.

5. The multiple modulus selector as recited in claim 2, wherein the modulus M is stored in a register.

6. The multiple modulus selector as recited in claim 2, wherein the modulus recoder further generates a multiple modulus negation indicating signal (NEG_MM) that is input to an accumulator.

7. The multiple modulus selector as recited in claim 2, wherein the n-bit modulus M includes a second least significant bit M[1] and a sum SPPI[1:0] of the previous sum and current partial product.

8. The multiple modulus selector as recited in claim 2, wherein the first selection signal includes two bits SEL_MM[1:0]

9. The multiple modulus selector as recited in claim 2, wherein the modulus selector further generates a multiple modulus accumulation indicating signal SEL_M2 that is input to an accumulator.

10. The multiple modulus selector as recited in claim 2, wherein the multiplicand includes two bits $SSPP_I[1:0]$.

11. The multiple modulus selector as recited in claim 2, wherein the second selection signal includes two bits SEL_M1[1:0].

12. A Montgomery multiplier comprising:

a multiple modulus selector for selecting one of –M, 0, M, and 2M (M being an n-bit modulus number) as a multiple modulus in an integer modular multiplication mode and selecting one of 0, M, and 2M as a multiple modulus in a polynomial modular multiplication mode to output a multiple modulus accumulation indicating signal SEL_M2;

a booth recoder for providing a first value used to obtain a partial product value; and

an accumulator for summing second values to obtain a result of the Montgomery multiplier,

wherein the accumulator sums the modulus M and the second values based on the multiple modulus accumulation indicating signal SEL_M2 in the polynomial modular multiplication mode.

13. The Montgomery multiplier as recited in claim 12, further comprising:

a modulus number register for storing a modulus value therein;

a multiplicand register for storing a multiplicand value therein;

a multiplicator register for storing a multiplicator value therein;

an AND gate for combining the multiplicator value with the multiplicand value; and

two adders for combining the values from the accumulator and the AND gate to output a combined value,

wherein the combined value is input to the multiple modulus selector.

14. The Montgomery multiplier as recited in claim 12, wherein the multiple modulus selector comprises:

a modulus recoder for receiving an n-bit modulus M, a previous sum, and a current partial product to generate a first selection signal;

a modulus selector for receiving the n-bit modulus M, the previous sum, the current partial product, and a multiplicand to generate a second selection signal; and

a multiplexer for receiving inputs –M, 0, M, and 2M and selecting one of the inputs based on the first selection signal in an integer modular multiplication mode and selecting one of the inputs 0, M, and 2M based on the second selection signal in a polynomial modular multiplication mode.

15. The Montgomery multiplier as recited in claim 12, wherein the booth recoder comprises:

a first selector for receiving a multiplicator to generate a third selection signal SEL_PP[1:0];

a second selector for receiving the multiplicator to generate a fourth selection signal SEL_A1[1:0]; and

a multiplexer for receiving inputs –M, 0, M, and 2M and selecting one of the inputs based on the third selection signal in an integer modular

multiplication mode and selecting one of the inputs 0, A, and 2A based on the fourth selection signal in a polynomial modular multiplication mode.

16. A modulus selector for receiving the n-bit modulus M, the previous sum, the current partial product, and a multiplicand to generate a second selection signal, comprising:

a modulus selector unit for receiving an n-bit modulus M, a previous sum, a current partial product, and a multiplicand to generate a selection signal, for selecting one of the three values 0, M, and 2M, that is input to a multiplexer and a modulus accumulation indicating signal that is input to an accumulator.

17. A booth recoder, comprising:

a first selector for receiving a multiplicator to generate a first selection signal SEL_PP[1:0];

a second selector for receiving the multiplicator to generate a seccond selection signal SEL_A1[1:0]; and

a multiplexer for receiving first inputs –M, 0, M, and 2M and selecting one of the first inputs based on the first selection signal in an integer modular multiplication mode and receiving second inputs 0, A, and 2A and selecting one of the second inputs based on the second selection signal in a polynomial modular multiplication mode.